CARTER, LEDYARD & MILBURN
COUNSELLORS AT LAW
1350 I STREET, N.W.
SUITE 870
WASHINGTON, D.C. 20005

2 WALL STREET
NEW YORK, N.Y. 10005
(212) 732-3200

114 WEST 47TH STREET
NEW YORK, N.Y. 10036
(212) 944-7711

(202) 898-1515
FAX: (202) 898-1521

July 7, 1995

RECEIVED
JUL 7 1995
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

BY HAND

Mr. William F. Caton, Secretary
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

Re: Petition for Reconsideration in
CC Docket No. 92-115

Dear Mr. Caton:

This is to provide notice, pursuant to Section 1.1206 of the Commission's Rules, that Carol A. Patton, President of C-Two Plus Technology ("C2+"), H. E. Cauthen, Jr., a C2+ consultant, Dr. Richard C. Levine, another C2+ consultant and the undersigned, as counsel for C2+, met yesterday with Blair Levin, Chief of Staff to Chairman Reed Hundt, Regina M. Keeney, Chief of the Wireless Telecommunications Bureau, and Steve Markendorff, Chief of the Broadband Branch of the Commercial Wireless Division. Michael Heavener, Vice President of the Independent Cellular Service Association, a trade association of emulation service providers unaffiliated with C2+, also attended the meeting.

The matters discussed were those contained in C2+'s Petition for Reconsideration and other submissions in the record along with the attached "Report on ESN Emulation and Cellular Phone Extension Service" prepared by Dr. Levine. Copies of Dr. Levine's Report were provided to Ms. Keeney and Mr. Markendorff and we respectfully request that the Report be made part of the record in the above-referenced proceeding. An original and two copies of this notice and the attachment are being submitted, but additional copies of Dr. Levine's Report can be provided if necessary.

If you have any questions regarding this matter, please contact me.

Very truly yours,

Timothy J. Fitzgibbon
Counsel for
C-Two Plus Technology

TJF:kdd
Enclosures
cc: Blair Levin, Esquire (w/encl.)
Regina M. Keeney, Esquire (w/encl.)
Steve Markendorff, Esquire (w/encl.)

Report on ESN Emulation and Cellular Phone Extension Service

by Richard C. Levine, Sc.D., P.E.
Beta Scientific Laboratory, Inc. and
Electrical Engineering Department,
Southern Methodist University,
Dallas, Texas

Introduction and Scope: I am a practicing electrical engineer specializing in the area of cellular telecommunications systems and a professor of electrical engineering and telecommunications. My educational background and professional qualifications are set forth in Exhibit 1. I have been requested by C-Two-Plus Technology, Inc., (C2+) to review several previous submissions before the Commission on the subject of ESN transfers in connection with cellular extension service, and in particular certain allegations against C2+ technology, to evaluate whether there are technological or system impact issues which should prohibit or restrict the use of such technology. In the preparation of this report I have reviewed the documents submitted to the Commission in CC Docket No. 92-115 which are listed in Exhibit 2 Documents noted with an asterisk are cited herein.

Summary of Conclusions: Based on my experience in the design and trouble-shooting of cellular systems and on review of the above materials I have concluded the following:

1. The problems of system burden to a cellular network alleged in several submissions do not exist in real practical cellular systems when emulated extensions are properly used (that is, only one of a multiple number of emulated extension mobile sets is powered up at a given time). There is no case of any burden or harm to the network or to other subscribers due to proper use of emulated extension cellular phone sets. There is no problem of incompatibility or interference with anti-fraud techniques in any case of proper use of emulated extensions.

2. Even in the case where multiple emulated extension sets are powered up simultaneously there are no extraordinary burdens

on the system. Air time is properly recorded and billed by cellular systems. The only potential problem arises where multiple emulated extension sets are used simultaneously, and a false alarm can occur in systems using a certain type of anti-fraud method (simultaneous or velocity checks). However, I wish to emphasize that this is a false alarm since no fraudulent use occurs. It is significant to note that there is no record of such false alarm conditions resulting in termination of service to any customers of C2+ emulation. The three other major anti-fraud methods (behavior pattern checks, use of a supplementary subscriber PIN, and RF signature methods) are not adversely affected. The actual problem area is not a technological one of false alarms for fraud (since actual fraud does not occur) but instead the problem lies with the carrier's policy and procedure in handling the false alarm like a true alarm. Even in this potential worst case the harm, if any, is confined entirely to the emulated extension customer, who is denied subsequent service under the operating policies of most carriers. In no case is there any harm to the network as a whole or to any other customers.

3. In my view, the use of emulated extensions provides a technologically superior method for providing extension service to those customers who desire extensions. The advantages of the emulated extension over services such as MUSDN relate to system simplicity, economy of resource use, and a superior level of service to the customer since all of the multiple emulated extension mobile stations are capable of roaming and temporarily selecting the competitive carrier, while all but one of the MUSDN-type extensions are not. There is no conflict between properly used emulated extensions and the four present anti-fraud methods, and emulated extensions can be adapted for IS-54B authentication. I conclude that the alleged conflicts between properly operated emulated extensions and anti-fraud methods, alleged added consumption of network resources, and/or impaired service or capacity to the emulated extension customer, to the network as a whole and to other customers, in the submissions I

have read and responded to, are incorrect and are based on incorrect statements concerning the actual current functionality of real practical cellular systems.

4. Neither the present wording of Rule 22.919 nor the proposed modifications suggested by the TIA and CTIA will advance the cause of fraud prevention nor inhibit fraudulent cloning of cellular telephone sets, but instead will deny legitimate uses of modified ESN such as emulated extension service and restoration of service to victims of fraud without change in directory number. The prohibition against changing the ESN and the three specific methods in the present wording for software treatment of the ESN do not technologically prevent or even significantly increase the difficulty of fraudulent "cloning" by criminals. Their only foreseeable effect on the industry is to prevent legal provision of emulated extension mobile stations, or replacement stations with the same MIN but new ESN for restoration of service to fraud victims.

5. Emulated extensions do not require the carrier to expend any resources for either initial activation or on a continuing or recurring basis for additional extensions. Therefore, there is no added recurring cost to the carrier to provide service to multiple emulated extensions. To preclude the potential false alarms which are an apparent concern to some carriers, I suggest as have others already, that the carrier identify emulated extension customers in systems which use "simultaneous" or "RF signature" equipment, and I agree that, the carrier should receive a reasonable amount as compensation for system resources used to store these bits. At the same time there should be corresponding safeguards to prevent abuse of the discretion of the carriers with regard to these activities.

6. Leaving the wording of Rule 22.919 in its present form, or including the changes suggested by the TIA and CTIA, would not address other known types of fraud and potential damage to the cellular network, since these wordings only address the ESN. Furthermore, these wordings will not stand the test of time, but would probably require repeated major modifications and additions

by the Commission as early as 6 months from today, due to technological changes which can be foreseen for cellular service and which are already available in the competing PCS-1900 and DECT systems planned for use on the 1.9 GHz PCS band. These new technologies allow the customer himself or herself to move the identification module (a removable computer chip which is analogous to, and in a US Cellular technology version actually contains, the ESN) from set to set, thus changing the ESN at will.

Report: In Section A of this report, I will first address the basic technological root of the significant cellular fraud problem now facing the industry. In Section B I will review the technological distinctions between the present MIN/ESN-based system of the 800 MHz cellular technology and the various second generation systems for authentication, particularly with regard to their bearing on the value of "hardening" of the hardware and software and their significance with respect to extension service. In Section C I will review the various allegations of network harm and the allegations of interference with present measures to combat fraud, and will consider the interaction of each method with regard to extension service. In Section D I will present my conclusions and recommendations.

A. Underlying Source of the Cellular Fraud Problem: The US cellular service clearly suffers from a large and constantly growing problem of fraud losses. The fundamental technological reason for this fraud is the use of an invariable identifier, the MIN/ESN pair, transmitted in "clear" form, as the basic method for identification of the mobile station. MIN/ESN identification is an inherently flawed method and all the resulting problems arise from this fundamental flaw and not from the capability to alter the ESN in other sets, contrary to the claims of other submissions. In contrast to other aspects of the US cellular system which are admirable in the aptness of their design to meet the present and future needs for performance and flexibility, the flaws in MIN/ ESN identification are fundamentally irreparable.

My carefully considered conclusion is that even in a hypothetical scenario in which absolutely all mobile stations in America were magically transformed to comply with the specific provisions of Rule 22.919, as strongly as a sincere manufacturer using the most "hardened" technology can achieve, this would only temporarily and only slightly decrease the amount of fraud, and then the rate of growth of fraud would continue as it does today. The three methods stated in Rule 22.919 do not significantly increase the technological difficulty for a criminal to change the ESN transmitted by a mobile set. This technological problem cannot be rectified by some more clever wording of Rule 22.919 to hide or sequester the ESN. Ultimately fraud will be undiminished. In other words, there is no light at the end of the tunnel if the only technological method of validation is the MIN/ESN identification process.

In my opinion, both the current and proposed wording of Rule 22.919 are misdirected when they prohibit changing the ESN, require that attempted modification of the ESN should make the set inoperative, specify who can or cannot change the ESN, or give specific requirements for software coding of the ESN. These requirements in FCC rules are like the legendary King Canute commanding the tides to flow backward. Every manufacturer can do the best possible design with the best available technology to meet these goals, but none of these things can be accomplished with any technology available today. If such a technology is developed in the future, then perhaps the current wording of Rule 22.919 regarding ESN would be meaningful and implementable. Categorically and without exception, every US analog cellular mobile station manufactured to date and currently in production using existing technology is susceptible to altering the transmitted ESN. The most hardened physical construction known would still not prevent transmission of an altered ESN. If the Commission desires a detailed description of several simple methods, already well known and readily available to criminals, which can defeat and/or bypass the specific hardware and software methods described or implied by the state of the art to conform

to the present Rule 22.919, a supplementary report can be provided. Such over-hardening only makes the mobile stations more expensive to manufacture, difficult or impossible to repair, and would even prohibit the retrieval and reuse of good components remaining in case of a partial component failure. But overhardening will not deter criminals with only a modest knowledge of technology. The problem does not lie with the construction of the mobile stations. The problem arises because the ESN must be used in the "clear." The TIA and other petitioners have recognized this underlying problem[1].

Furthermore, there is a wrong-headed emphasis on only the ESN, when a number of other parameters of the mobile station can also be modified to produce fraudulent or other damaging effects with or without changing the ESN. As each new method of fraud becomes widespread, will the Commission be required again and again to constantly rewrite Rule 22.919 and other relevant sections to cover new circumstances which can be foreseen technologically now and covered by a properly drafted rule, but which are not yet widely used for fraud?

B. Improved Authentication Methods Do Not Use MIN/ESN Validation: Designers of all "second generation" cellular and PCS systems have recognized the fundamental deficiency of the MIN/ESN identification method for billing authentication or identification, and consequently have not used it. The Ad-Hoc Authentication Group (AHAG) of the TIA TR45 standards committee at first directed serious effort to search for any possible method to provide positive authentication by continuing to use the ESN. This was viewed as very desirable by the carriers' representatives to the standards committee, since it would not require any changes in operational procedures. However, after careful study, that group agreed that the ESN method was neither theoretically nor practically acceptable as the basis of an authentication process. Based on information conveyed to me in a

---

[1] TIA Stay Dec. '94, pp. 5-7 and p.11, and TIA Clarification Dec. '94 pp. 5-11 and p. 13.

meeting with the chair of the corresponding European Telecommunications Standards Institute (ETSI) committee, ETSI also went through the same process. As a result of such study, use of the ESN was abandoned for verification. All the second generation cellular and PCS equipment in both America and Europe uses an algorithm similar in principle to that in TIA IS-54B, but different systems differ in details of implementation. The experience to date with these systems in Europe fully proves that such an IS-54B-type authentication system is technologically fraud-free. Criminals have only been able to commit fraud against such new systems via non-technological means such as subscription fraud.

All second generation systems involve three essential authentication steps First, a "challenge" number is transmitted from the base to the mobile station. Second, the mobile station then uses an internal secret number and this challenge value to calculate a response value, which is transmitted back from the mobile to the base station. Third, the base station compares the "correct" response value to the value returned by the mobile set, and can thus determine if the mobile station is authentic or not. This knowledge of the correct response comes ultimately from another copy of the secret number of this particular mobile station, in an appropriate part of the overall cellular network. Because the same challenge value is never repeated in a manner useful to a criminal, and the secret number remains secret (since it is never transmitted outside the mobile station and the appropriate parts of the cellular base infrastructure in the "clear"), a criminal cannot successfully imitate the authentic mobile station.

Second Generation Systems Allow "Extensions" with the Authentication Data Analogous to the ESN to be Moved From One Set to Another by the Customer. The European system designers knew from the start that one of the desirable marketing features required in a modern cellular system is the ability for the customer to use various so-called "extension" telephones in different locations and circumstances. The second generation

systems developed in Europe are therefore explicitly designed to allow transfer of the authentication module, analogous to but more secure than the ESN of the US cellular system, from one mobile station to another. These European-developed systems in particular include the Global System for Mobile communications (GSM), the Digital European Cordless Telephone (DECT), and others.

The authentication module is preferably implemented as a small silicon chip called a subscriber identity module (SIM). Unlike the MIN/ESN identification method, the SIM chip can be manufactured in a realistically hardened form (microprocessor and data memory in the same silicon chip with no accessible internal connections) which is a true protection against physical access compromise of the mobile station. The whole problem of trying to prevent change of the data (analogous to the ESN for identification) in the SIM chip has no impact on fraud prevention, because the system design stops the problem at the source: 1) The secret information cannot be intercepted via the radio signals; 2) The secret information cannot be extracted from the chip physically by any means accessible to unauthorized parties; and 3) Anyone can easily change the information in the SIM chip (secret and otherwise) with readily available computer equipment, but this does them no good if they don't have the proper secret numbers. Compared to the situation in the US cellular system, the actual cause of the problem has been identified and cut off at its source: one cannot learn the secret identification number hidden in the mobile station (actually in the SIM chip) by any means available to unauthorized third parties.

This SIM chip for second generation systems may be packaged in either a small plastic chip carrier, smaller than a child's fingernail, or it may be incorporated into a so-called "smart card" which is similar to a credit card with electrical contacts. This chip can be moved by the customer at will from one mobile station to another. A customer thus has the ability to use the same identification in multiple handheld portable set(s), and

vehicle-mounted set(s) with higher power, and public vehicle-mounted sets installed in a taxicab or bus for the use of the public, and in a rented mobile station. The carrier is not burdened with special billing procedures (which are more costly and complex) when the customer temporarily uses a different mobile station.

The leading technology in terms of installation plans in the USA for the 1.9 GHz personal communication system bands auctioned by the Commission this winter is the so-called PCS-1900 system, which has the same features described in the previous paragraphs for GSM. Other systems put forth by manufacturers for the 1.9 GHz band have such a feature as well. The PCS-1900 equipment is ready now, since its design and debugging was done very fast by incorporating the GSM technology which had already gone through the initial debugging stages. I have personally worked with two manufacturers who have equipment ready to install and are now training installation teams. Service may begin on some of these systems in less than 6 months.

Relevant Features of PCS and US 800 MHz Cellular. This table compares the relevant features of US 800 MHz cellular and a typical second-generation system for providing extension service. The three columns describe, respectively, US cellular service under the present rule 22.919 with extensions provided by a MUSDN[2]-like service offering, US cellular with C2+ or other emulated extension mobile stations, and a second generation system such as GSM or PCS-1900.

---

[2] This is a marketing name for "Multiple Units- Same Directory Number." Other marketing names for essentially the same marketing package include "2 Phones/1 Number" and "FlexPhone." It is described in more detail at pages 15-17.

Relevant Feature	Rule 22.919 Jan'95 & Proposed changes (with MUSDN exten's)	Emulated Extension such as C2+	GSM and PCS-1900 et al
Physical hardware package of identification information	ESN hardware must be physically attached to main circuit board, non-removable. Each mobile must have a different ESN	Same MIN/ESN in multiple mobile stations	Authentication module is designed to be removable by customer
Permitted portability	Only one ESN uniquely attached to one mobile station	Only one station usable at a time to avoid false simultaneous checks.	Authentication module may be moved by customer to any mobile station
Who can move identification?	Manufacturer or authorized representative only. Customer is prohibited.	Customer orders from technician.	Customer or any person with the authentication module
Billing complexity	Each mobile station is treated separately, and requires system overhead of a separate customer; or a secondary billing (e.g. credit card) must be used when customer uses an alternate mobile station . MUSDN billing combines separate station detail records into one presented bill.	No increase in billing complexity compared to one mobile station	All mobile stations are treated as the same customer, and use the system overhead of only one customer. No separate or supplemental billing methods are required.
Security against fraud	Poor experience Invariable MIN/ESN method is fundamentally flawed. Many "successful" criminal fraud methods	Emulated extension sets are no more and no less susceptible to fraud than a single station set.	Excellent experience. Use of same authentication in different sets does not compromise authentication because algorithm is fundamentally secure.
Roaming Capability	Only first MUSDN set can roam. Other MUSDN sets cannot be given service while roaming or in areas covered best by alternate carrier at home	All extensions have full roaming capability	All extensions have full roaming capability

Meets customer/ system economy and service needs?	Not well. Customer pays almost double cost for two extensions via MUSDN-like service, and carrier has double system overhead.	Fully meets customer needs for inexpensive extension service. No added system resources required for emulated extensions.	Fully meets. Customer pays same monthly cost for one or an unlimited number of mobile stations. System overhead is not increased regardless of the number of sets used. European carriers charge supplementary fees for roaming to other cities, but not for use of additional mobile stations.

Some of the technological considerations underlying the statements in this chart are discussed later.

Please note that an IS-54B authentication module, suitably packaged in one "hardened" chip (like a SIM chip), is technologically capable of providing all the same extension and superior authentication features to US cellular carriers and their customers as are enjoyed by users of GSM and PCS-1900, but this is legally prohibited by the present Rule 22.919! It is also significant to note that all the benefits cited for multiple mobile station use (particularly the advantage of no added system overhead) can be delivered today in the US cellular system using ESN emulation, and the level of fraud protection depending only on the ESN is no better and no worse than a single US mobile station. If Rule 22.919 were to be re-written so that an IS-54B authentication module (and thus the ESN, which is inside such an authentication module or chip in the IS-54B standard) were to be legally permitted to move from set to set by the customer, then all the benefits shown in column 3 can be delivered to a US cellular carrier and customers well. The present and proposed wordings of Rule 22.919 not only inhibit technological progress, but also have the effect of prohibiting the most technologically

simple method for customer extension service and driving the legitimate providers of emulated extension mobile stations out of business.

Although statements have apparently been made to the contrary in the industry and have been repeated in previous Commission comments[3], it is technologically feasible to have multiple emulation extension stations with the same IS-54B authentication, by two methods. One of these methods requires no modification in the present IS-54B standard but only a procedural change, and the second method requires only one or two reserved bits to be assigned to distinguish the several emulated extension sets. Since other upgrades to IS-54B authentication are also desirable at this time, one of these methods can be viewed as currently available and the other method can be viewed as possibly soon available under a standard. The details of these methods can be described in a separate sealed submission upon the request of the Commission. This topic will be again discussed in more detail with the response to alleged network harm, but the use of two or more sets with the same IS-54B identification is superior with respect to network resources and overhead compared to the MUSDN-like method. In the technology using a SIM or SIM-like (IS-54B) chip, all the mobile sets used by the same subscriber can roam with equal ease. Once the new PCS technology is competing in the USA with 800 MHz cellular for the same customers, it is likely that the 800 MHz cellular carriers will want a reversal of Rule 22.919 to explicitly allow movement of the ESN from set to set at the will of the customer, permit the ESN to be easily removable from the set, and so on.

C. Review of Arguments Against Use of Emulated Extensions:

It is not practical to quickly change or replace all mobile stations already in the field to an improved method of authentication. MIN/ESN-based identification will be with us for several years to come. A practical program is necessary to reduce and eliminate fraud which does not misdirect scarce anti-

---

[3] Report and Order Sept.'94, paragraph 59.

fraud resources in wasteful ways, and which does not prohibit legitimate and beneficial consumer services and capabilities which utilize ESN transfer. The Commission should preserve the benefits available to consumers from authorized ESN transfers and prohibit only those ESN transfers which are done for fraudulent use. Proponents of the present and the TIA/CTIA proposed wordings claim to do this, but in fact they do not.

Carriers have raised two arguments against the use of emulated extension use. First, they claim that such use contributes to cellular fraud or undermines their methods for combating fraud. Second, they argue that such use creates operational problems or burdens on the network. In this section we examine each type of argument.

Cellular fraud involving a MIN/ESN-identified mobile station consists of two steps: 1) unauthorized interception of ESN and MIN, and 2) fraudulently placing that ESN and MIN in another mobile station. It is significant that all prior petitioners whose submissions I have examined have focused <u>exclusively</u> on step 2. There are several valuable and useful actions to detect, prevent, confound and inactivate criminal activities at step 1. They may not be the direct responsibility of the Commission, <u>except</u> to the extent that <u>active</u> interception of such information involves radio transmission by the criminal to interrogate the mobile station. Such transmissions which have the motive of fraud should be identified by rules as illegal <u>regardless</u> of the low power level used. They should be clearly distinguished from valid use of the same equipment for test purposes. I can address this in a separate submission to the Commission, if desired. Additional specific anti-fraud actions against step 1, which are effective against <u>both</u> active and passive interception of MIN/ESN pairs, are not described here because their description in a public document would aid criminals' evasion. These steps to combat interception of the MIN/ESN pairs have frequently been overlooked or under-utilized by the industry, and this is mentioned because they illustrate what has been properly called

"one-dimensional" thinking[4] in the industry concerning the fraud problem.

The cellular carriers have focused their attention and that of the Commission only against step 2, and in doing so some have opposed modification of the ESN in the mobile station as though it were the only way to achieve fraud protection, although changing the ESN has many important legitimate uses such as emulated extension mobile stations, substitution of a replacement for a faulty mobile station, correction of firmware/software flaws in the field, restoration of service to victims of fraud, and general repair of mobile stations. Furthermore, there are several methods for fraud which do not utilize ESN transfer at all. The proposed wording change to the January Rule 22.919, which permits only the manufacturer to modify an ESN, is an unsatisfactory and ultimately futile approach to the true requirements of effective fraud control and capability to provide fully competitive features, as already explained. I am very unhappy to find that so much of the Commission's time has been directed to the details of attempting to "harden" the ESN, and in prescriptions regarding who should and should not be permitted to change the ESN, and in attacking emulation providers in particular, rather than more technologically and practically productive approaches. Many claims were put forth by cellular carriers which can be characterized as follows:

1. Claim(s) of generalized network harm without explanation or substantiation;

2. Claim(s) of specific network harm which, in fact, is/are factually incorrect;

3. Claim(s) of specific network harm which, in fact, could only occur due to improper or inadequate operation of the network by the carrier;

4. Claim(s) of specific network harm which, in fact, already arise(s) today from sometimes unavoidable problems in

---

[4] This "one dimensional" characterization has already been given to this situation in CTIA Opposition Jan. '95, p. 7.

network design and/or operation, regardless of the presence or absence of emulated mobile station in the network;

5. Claim(s) of general network harm from a specific cause when in fact the cause cited would only affect the individual customer whose mobile station is emulated, and not the entire network or any other customers;

6. Claim(s) of certain general or specific network harm which is/are inconsistent with other general or specific claims by or logically inferred from claims of the same petitioner or other petitioners or of other industry sources;

7. Claim(s) of specific network harm which could only arise from refusal of the carrier to work equitably and cooperatively with information from the providers of emulation, in other words a "self-fulfilling prophecy" or a problem generated merely for the sake of prolonging the argument rather than a valid objection; and

8. Claim(s) of loss of revenue. This revenue, in the form of either air time (which is, in fact, always billed properly for emulated extensions and is not lost) or so-called initial "activation" or some recurring charge for additional units, is alleged to be inherently deserved by the carrier. This is an economic issue, and public utility economics is outside my sphere of expertise. However, there is an underlying claim in these cases that there is added consumption of network resources which must somehow be compensated, which I <u>can</u> address.

To avoid repetition, I will refer in future to these numbered descriptions to shorten the discussion of each claim, by means of a table with a check mark for each applicable description.

Carrier Extension Service Offering via MUSDN. Recognizing the desire by customers for extension service, some carriers have put forth a service marketing offering often called MUSDN. (I use this particular marketing term - defined in a previous footnote - here only because it is the shortest marketing name for this service package) Different MUSDN "extensions" have the same MIN but a distinct ESN in each such mobile station unit.

Some prior submissions claim that MUSDN is superior to emulation[5]. I will address this claim with regard to various specifics where appropriate. However, in general, MUSDN requires modification of the data base software in a number of parts of the system and network software to handle multiple entries with the same MIN. Otherwise, the multiple MUSDN mobile stations are treated as distinct mobile stations by the system. This implies that the overall data storage and system operations for multiple MUSDN station sets are as much as or greater than an equal number of unrelated separate mobile stations. To initiate service, each additional MUSDN mobile station requires all of the same activation operations in the carrier's technological switching and infrastructure and business and clerical operations as a new unrelated mobile customer. The ongoing resources required for each MUSDN mobile station with regard to computer memory, computer internal operations and messages, etc., are respectively equal to that of a separate mobile station.

However, despite all of this consumption of system resources, the customer does not have access to all system facilities. In general, only one of the multiple MUSDN station sets for a given subscriber (i.e. the "primary" phone) is able to roam, because the home system data base refuses to acknowledge the other MUSDN sets as valid customers according to established policy of the cellular carrier. This also leads to other restrictions on the customer in the home service area, some of which can run counter to existing FCC directives.

In contrast to this, emulated extension service via multiple mobile stations having the same MIN/ESN identification are treated indistinguishably by the cellular network, as most petitioners and the Commission itself have already observed. There is no technological distinction between the various mobile stations held by the same customer, and all can have roaming service. There is consequently no restriction of service and particularly no restriction on roaming or home area calls via the

---

[5] McCaw Comments Jan. '95 p.13.

local alternate (A vs. B) carrier, which is one of the serious technological shortcomings of MUSDN (to be explained). If the customer takes reasonable care to use only one emulated extension mobile station at a time, there is no consumption of network resources beyond that of one mobile station alone. This specifically implies that there are no costs or resources expended by the carrier to activate additional emulated extension mobile stations, and there are no initial activation operations or data entries, no ongoing, recurring or continuing resources such as computer memory, internal computer operations or messaging, or the like. For this and other reasons, I therefore conclude that MUSDN is actually not superior as measured by network resources consumed and limitations on service to the customer, and can even be described in several ways as inferior or "substandard" compared to emulation. The claims that emulated extension mobile stations conflict with anti-fraud measures will be discussed point by point later.

Specific Allegations Analyzed: In many cases I will provide a significant level of background detail to substantiate my conclusion. Also, a point of confusion emerges as one reads the previous submissions. An emulated extension mobile station can be used properly, with only one station at a time having power on, or improperly with multiple emulated extensions operated simultaneously. In many cases, complaints are made which appear to assume, contradictorily, that the emulated extensions are properly operated, which is a condition undetectable to the cellular network, and also improperly operated, which may cause false alarms for simultaneous activity. I have tried to carefully distinguish these two conditions and to evaluate the relative effect on the individual extension phone user and on the system as a whole. I have summarized the effects in a chart including the four distinct combinations of cause and effect, where it is appropriate.

Claims of "Rip Off" of service: McCaw[6] complains that the integrity of the system itself is undermined by the "deception" allegedly due to emulated extensions. They claim that the carrier and its entire body of customers bear the resulting direct and indirect costs. McCaw also claims that emulation extensions "rip off" cellular carriers and their subscribers. However, in all cases, without exception, cellular systems bill air time accurately for emulated extension mobile stations regardless of any specific features of the particular system. There is absolutely no circumstance to my knowledge in which a cellular system will not automatically and properly bill the customer for air time on any or all of multiple emulated extension mobile stations. In addition, the internal network resources, such as system memory, system processing, internal data communications activity and billing, are the same for multiple emulated extensions as for a single mobile station. This implies that the emulated extension is actually a more efficient (from the point of view of network resources) way to support two or more extensions than the MUSDN-like service offering.

Allegation of "rip-off"	Properly Used Extension	Improperly Used Extension
Effect on the emulated extension user	Air time is correctly billed. Customer also pays one monthly base fee.	Air time is correctly billed, even (when network allows) two simultaneous calls to occur.
Effect on other customers and the cellular system	Air time of extension subscriber is paid. Internal resources of network are no greater than for one mobile station. No effect on others and on system	Air time of extension subscriber is paid. Internal resources of network are no greater than for one mobile station. No effect on others and on system

I see no explicit claim or allegation in the prior submissions which I have read that emulated extension customers are evading payment of air time. There is therefore an implied

---

[6] McCaw Comments Jan.'95, p.8.

allegation that there are other operational or internal costs which the emulated extension customer is somehow evading. Again, it is significant to note that properly used multiple emulated extension mobile stations are indistinguishable from a single mobile station, as already effectively stipulated by everyone who has commented on this topic, and apparently accepted by the Commission as well. The underlying technological reason is that the actions in the network for the two contrasting cases are indeed absolutely identical. There is no added system hardware, software or memory, software development or design effort, messaging, billing or other network or operational resource which is greater for properly operated multiple emulated extensions than for a single mobile station. Despite this lack of underlying cost basis, some carriers may hold the view that they are entitled to an additional payment because of their public utility standing or some other non-technological basis, but I cannot comment on this as a technological expert.

In contrast to the identicality of resources for multiple emulated extension mobile stations, multiple extensions provided via the MUSDN type of service basically use all the system resources which are required for multiple sets which have distinct MIN directory numbers. In addition, special software development and testing is required, more system memory is needed since each mobile station is treated as distinct and uses the same system memory as an additional separate set, there is additional messaging in the cellular network, special billing consolidation is required, and this also requires development and testing of relevant billing software.

After all of this, MUSDN restricts the customer so that only one of the multiple mobile stations has full service capability and can roam to other systems. This creates a significant problem because many customers frequently drive in areas where their home carrier has poor radio coverage[7], but the competing (A

[7] The standard industry design goal is 90% or better radio area coverage in each cell. In some cases this goal is exceeded, but many systems have radio shadow areas due to obstacles between the base antenna and the mobile.

vs. B) local carrier has better radio coverage, or they are in a suburban area where the geographically irregular radio coverage boundary of their home system meets a suburban system. As they drive along a highway, for example, they are continually entering and leaving their home system radio coverage, which implies that they will not be able to begin a call (either originate or answer) part of the time in a highly unpredictable way. The previous 1985 order of the Commission which gives the customer the right to temporarily select the alternate (A vs. B) competitive carrier[8] is technologically nullified by the carrier's policy of not supporting roaming verification for any but the first MUSDN set. Finally, it is the practice of most carriers who offer a MUSDN type service to charge the customer approximately the same basic monthly price for each of the multiple station sets as they would charge for unrelated separate station sets.

Thus MUSDN can be characterized as inferior to emulated extension service from several technological and service points of view, and clearly does not meet the customer's concept of lower cost extension telephone formed from the analogous situation in landline telephone service where customer-owned extension telephones have been without extra monthly fees for over 20 years. There is a close analogy between emulated extension mobile stations and landline (wire telephone) customer-owned extension telephones. Neither one requires any additional resources on the part of the carrier either for initial activation or continuing service. They are not completely technologically analogous in their operation, because multiple mobile "extensions" cannot simply enter into a "conference" call," as wire extensions do, by merely lifting the handset. The cellular system requires a conference bridge (a special piece of

---

[8] Amendment of Part 22 of the Commission's Rules. CC Docket No. 85-25, 59 RR 2nd. 209, 1985.

hardware in the central cellular switch) to connect multiple stations (whether MUSDN or emulated extensions) in the same connection[9].

Alleged "rip off"	1✓	2✓	3	4	5	6✓	7	8✓

(See pp. 14-15 for explanation of chart).

Allegations of "Substandard" Service: McCaw[10] claims that emulation is a "substandard" service which its users do not pay for. To reply, first, we repeat that the air time is correctly billed as discussed previously, so that the customer pays for what he or she uses. Regarding the claim of "substandard" service, it is not possible to identify from the complaint specifically what part of the service is allegedly substandard. The interaction between the network and an emulated extension mobile station is, as other petitioners have correctly stated, indistinguishable with regard to differences between the first mobile station of a specific customer and other emulated extension stations. The quality of voice is identical in both cases. The quality of voice for other customers using the cellular network is identical for both cases. The carrier controls access of the mobile station to the voice channels. No excessive voice traffic usage can occur due to the presence of the emulated extension, and thus no radio interference can occur in a properly designed system. Radio interference can only occur if the system design is defective due to such reasons as inadequate or defective radio antenna coverage by the base radio (the mobile radio antenna is omnidirectional and does not control radio coverage). All of these things are within the responsibility of the carrier, and if these defects are present,

---

[9] In this regard cellular service has a similar complexity to integrated services digital network (ISDN) wire service, which is also not inherently capable of conferencing multiple wire connected extensions on the same subscriber loop, without use of a conference bridge in the central switch. The Commission specifically allows the ISDN customer to own and connect multiple ISDN station sets to the S interface without extra charge, even though the carrier must provide a conference bridge to permit two ISDN extensions to participate in the same call.

[10] McCaw Comments Jan. '95, p.12.

they will cause degradation to all customers in the defective cells, and have no relation to the presence or absence of emulated extension mobile stations.

The amount of voice and signaling traffic generated by a customer making a given number and length of calls is identical whether that customer makes all the calls using one mobile station, or in the alternative case when that customer makes those calls properly using two emulated mobile stations, one at a time. Even for improper simultaneous use of two emulated extensions, there will be no radio degradation in a properly designed system and all air time is properly billed as previously described. Therefore the quality of the service and the effect on other customers and the network are precisely the same. Again, this is a case where McCaw has claimed on one hand that the emulated extension cannot be distinguished from the first mobile station by the network, yet also claims to the contrary that deleterious effects occur to the emulated extension subscriber or others.

McCaw[11] also alleges that when two mobile stations respond to a page, the system does not know to which one to deliver the call, and this constitutes degraded service. In all cases which I am familiar with where cellular systems do permit multiple paging responses from either emulated extensions or MUSDN like multiple stations, there are three very definite algorithms in use, which do not leave any question unanswered regarding which station to deliver the call. One method is to deliver the call to the first mobile station response which the network receives. This method has some different variations regarding treatment of the other station. The second method is to ring both stations, and connect the caller to only the first one on which the customer answers. The other then ceases to ring. The third method is to designate only one MUSDN-like station as the primary one to receive calls. This third method has the deficiency that the pre-designated station is not necessarily the one desired by

---

[11] McCaw Comments, Jan. '95, p. 12.

the caller. Furthermore, when roaming, only one MUSDN station can receive calls. I know of no system in which there is any ambiguity or degradation of service because of two or more stations responding to the page for a single MIN. In view of the many services denied or prohibited to all but the first MUSDN station set, we could aptly describe MUSDN as "substandard" service.

Furthermore, there is a problem in many cellular systems which is aggravated when many small cells are used in, for example, a downtown area with high traffic. This problem pre-dates and has nothing to do with the entire issue of emulated extension mobile stations, but is still very much with us today. In certain locations, a mobile station transmitting an access message on the reverse control channel may be received by two different base stations (cells) using the same control frequency channel. As a further protection against this false double response, the cellular system normally includes a so-called 7-bit binary "coded digital color code." Despite this added protection, the system still receives double page response or setup messages in some cases. This problem is physically due to a combination of undesired but difficult to avoid antenna back- or side-lobe directional sensitivity, combined with the multiple wave reflections which exist in a cluttered urban environment. These together create a "sneak path" for radio waves to propagate to the wrong cell from certain particular locations. This unfortunately far too common problem indicates 1) the problem of multiple page responses cited is not always due, or not only due, to the presence of emulated extension mobile stations (in my own experience, it is almost never due to that), and 2) the antenna coverage and reflected wave problem, where it exists, is the responsibility of the carrier to correct, and would affect all mobile stations which happen to be in the bad propagation regions. The radio sneak path also creates false alarms for anti-fraud simultaneous and velocity checks for single mobile